EMBEDDED LINUX CONFERENCE

@

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
EUROPE

From A Security Expert's Diary

DOs and DONT's When Choosing Software for Your Next Embedded Product

Marta Rybczynska

Security Lead, Eclipse Oniro Project for Huawei OSTC

#ossummit @twitterhandle

THE LINUX FOUNDATION

Day 1

A product

DEFINING A PRODUCT: HARDWARE SUPPORT

- SOC (System on Chip) vendor support :
  - The SOC itself – is support in Linux mainline ? Device trees ? Quality ?
  - Peripherals – do they have upstream drivers ? Vendor's drivers (which version) ? Quality ?
- Is it supported by distributions/distribution building tools ?
  - Eg. is there a well supported Yocto layer ? Quality : passing yocto-check-layer ?

DEFINING A PRODUCT: FEATURES

- Network access
  - Which protocols ? Can they use encryption/authentication by default ? Eg. Default to TLS 1.2 or 1.3
  - Cloud functions ? Does it transfer user's data ? How will be the data protected ?
- APIs
  - Which libraries/APIs are must-have ?
- Support : how long ?
  - A typical product consists of hundreds of packages

Day 3

Distribution choice

SAY NO TO Do-it-yourself

DISTRIBUTION CHOICE

- Maintenance
  - Do they release security updates ? How frequently ? Are there long-standing security issues ?
  - How long is a version supported ? Do they have a Long Time Support version (LTS) ?
- Binary/source ?
  - Depending on your needs
  - Source : Yocto Project and derivatives (eg. Poky, Oniro), Buildroot
  - Binary : Debian, Ubuntu..

EXAMPLE: YOCTO PROJECT RELEASES

- https://wiki.yoctoproject.org/wiki/Releases

Codename	Yocto Project Version	Release Date	Current Version	Support Level	Poky Version	BitBake branch
Langdale	4.1	October 2022		Future - Support for 7 months (until May 2023)	N/A	
Kirkstone	4.0	May 2022	4.0.3 (August 2022)	Long Term Support (minimum Apr. 2024)	N/A	2.0
Dunfell	3.1	April 2020	3.1.19 (August 2022)	Long Term Support (until Apr. 2024)	23.0	1.46

Day 17

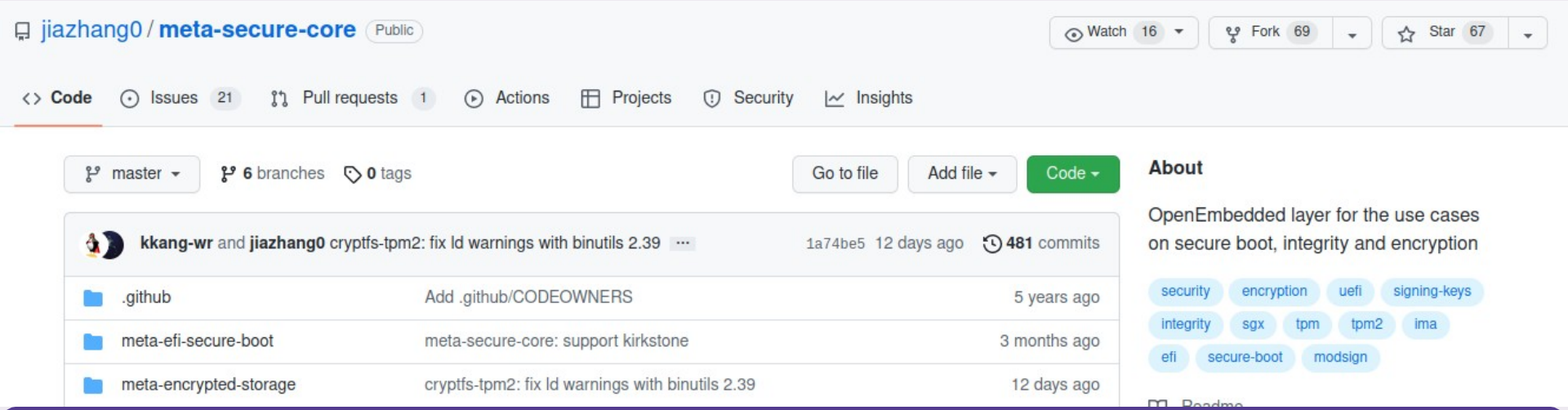
Layers bring layers bring layers bring layers

LAYER DEPENDENCIES: YOCTO PROJECT CASE

- Easy to add layers...
  - Harder to remove what you do not need
- Advice
  - Do you need all those layers ?
  - What is their quality ? Yocto Project Compatible ?
  - Is it maintained ?

DEPENDENCIES: AN EXAMPLE

- An included layer requests: https://github.com/jiazhang0/meta-secure-core



Day 27

A little package...

KNOW WHAT YOU HAVE

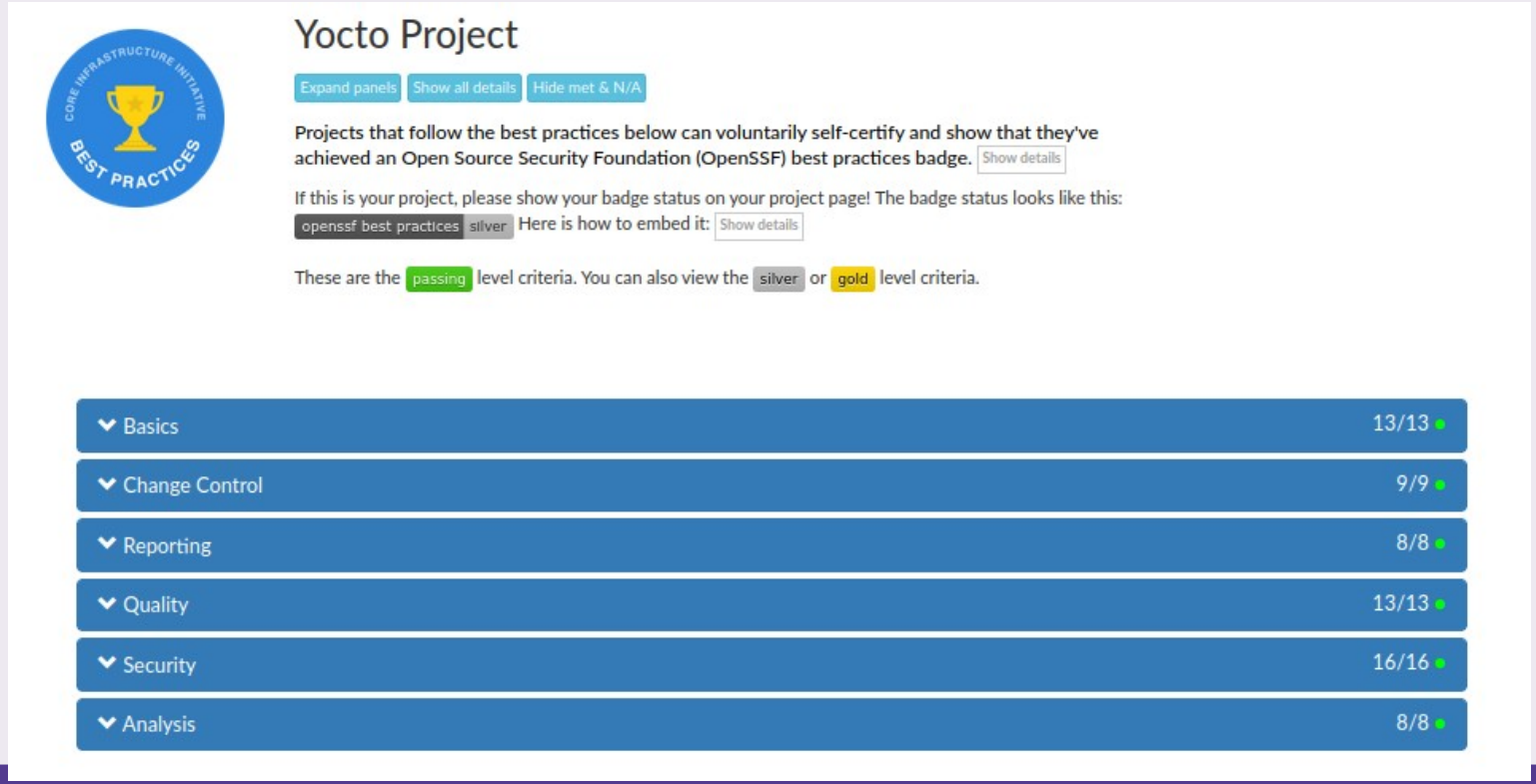
- Do you know how many components your project has ?
- Advice ?
  - Check your package list from time to time
  - (When using YP) Use and monitor results of:
    - bitbake -g (dependency graph)
    - cve-check (known security issues in your image)
    - create-spdx (create Software Bill of Materials)

EXAMPLE: DIGGING DEEPER

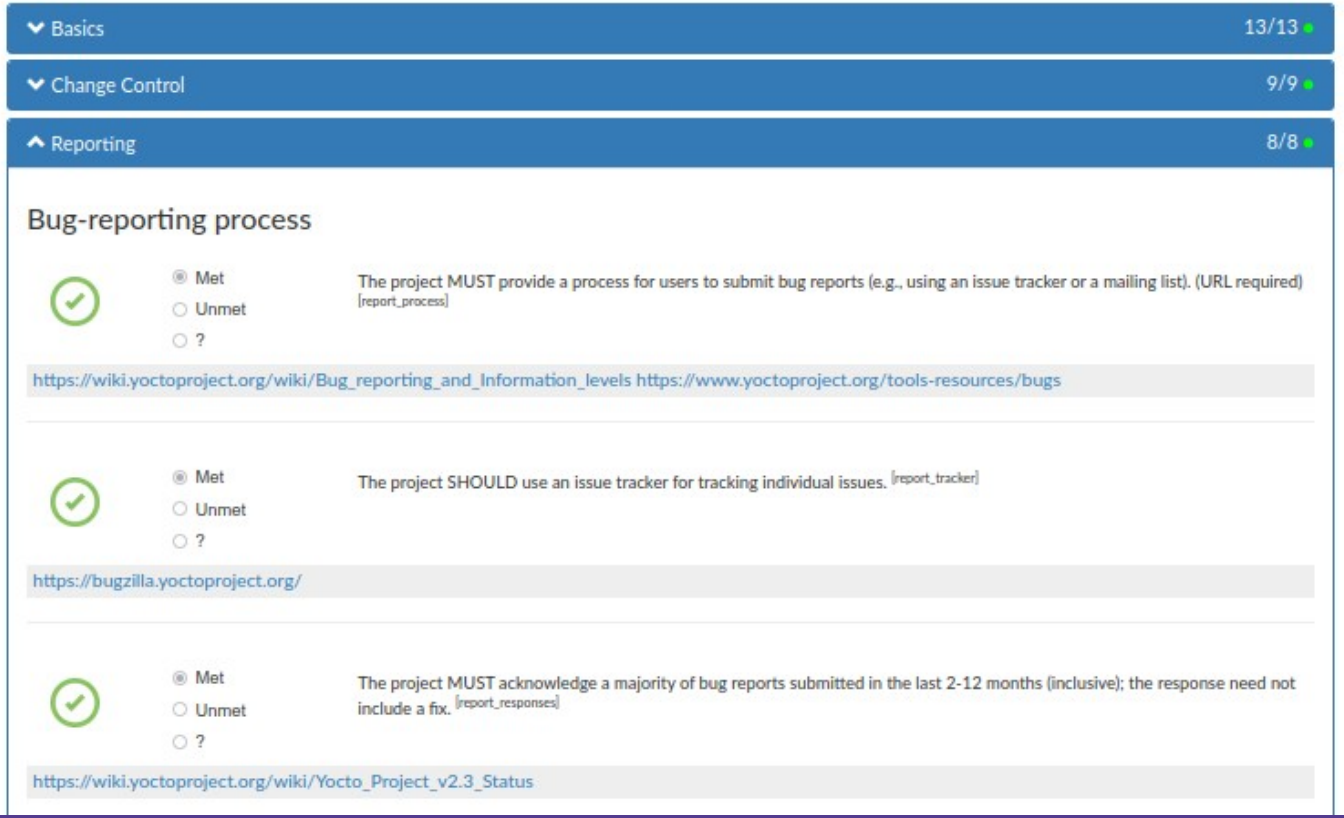
- Found libmicrohttpd in the package list
- Dependency chain :
  - Crypto libs→libmicrohttpd→debuginfod (from elfutils)
- Fixing :
  - Need to disable a configuration option in elfutils
  - In YP : via DISTRO_FEATURES

EXAMPLE: USING BEST PRACTICES BADGE (1/2)

- https://bestpractices.coreinfrastructure.org/en/



EXAMPLE: USING BEST PRACTICES BADGE (2/2)



Day 79

Updating now and forever

Day ~~7~~ → 11

Updating now and forever

UPDATING DEVICES

- Critical
  - Even in best design, there will be bugs (in your code, dependencies, or dependencies of dependencies)
  - Update is usually the ONLY way to solve the issue
- Know your update system scope
  - Firmware
  - Bootloader(s)
  - Kernel
  - Applications

Day ??

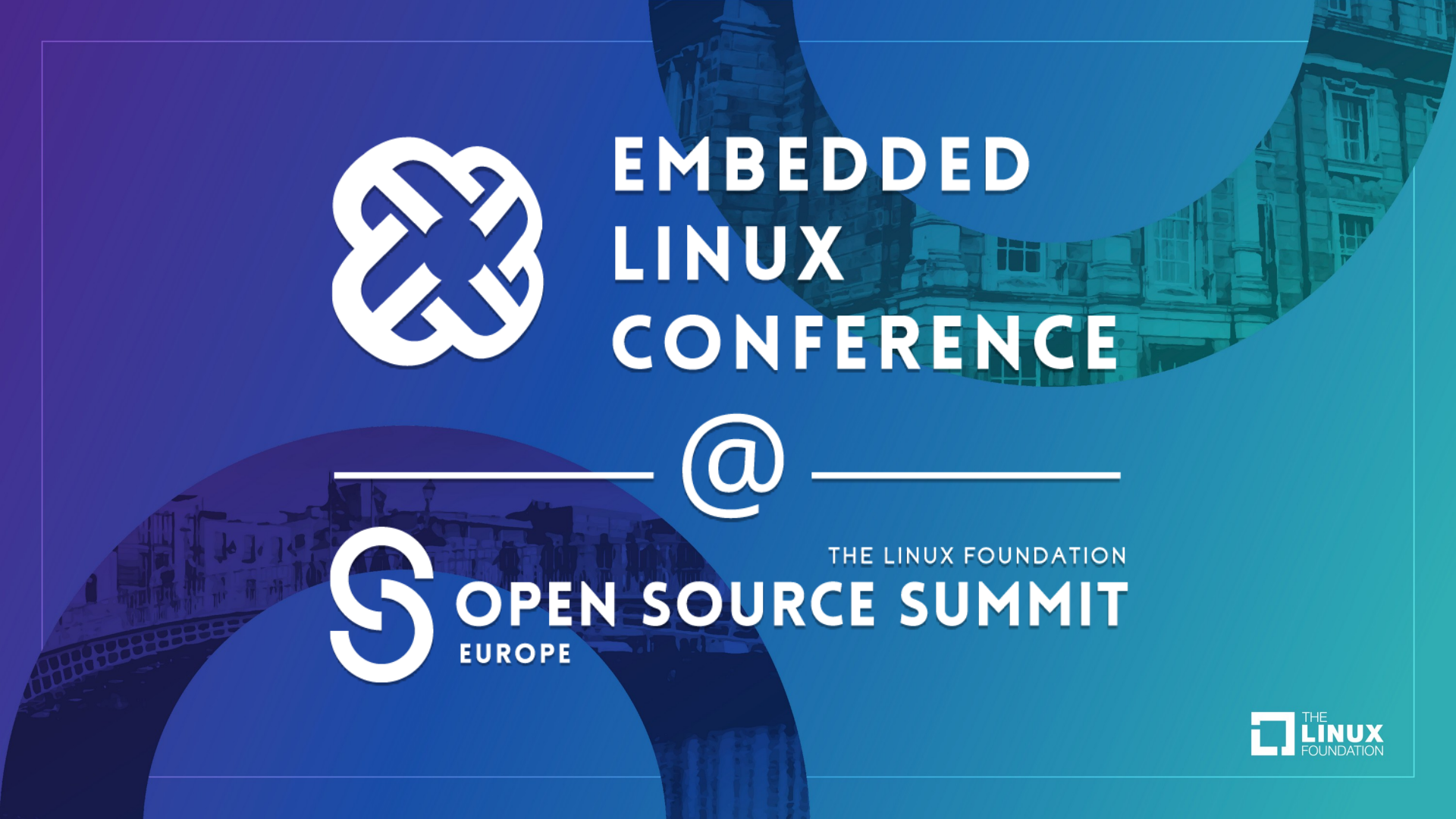
What next ?

MORE STORIES (for part 2)

- Secure boot
- Setting up your network protocols
  - DIY network protocols
  - Disabling/enabling encryption
- Updating Board Support Package (BSP)
- Backporting security patches
- Security Response Team

TAKE-AWAYS

- Good product security is like healthy living
  - Hard to add later
  - A number of small easy steps
- Evaluating your software is key
  - Do you need it ?
  - Is it good quality ?
  - Does it have security updates ?


EMBEDDED
LINUX
CONFERENCE
@
THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
EUROPE
THE
LINUX
FOUNDATION